



The Investigation, Implementation and Mitigation of Recent Cyber Exploits

By Daniel Carlson (2001079) - BSc Computer Networks and Cybersecurity

Project Supervisor - Dr Nitheesh Murugan Kaliyamurthy

Email: 2001079@student.uwtsd.ac.uk



1. Introduction

The strategy, significance, and comprehension of cyber-defence and its results are increasingly becoming paramount in today's technological age. It's critical to know the defining characteristics of the cyber domain to comprehend the dynamics of contemporary cyber assaults completely.

The relationship between individuals and modern human technological achievements is continuously expanding, including using modern technology to commit crimes and encourage crime worldwide.

[1]

2. Aim and Objectives

Aim

To investigate the recent cyber-exploits on simulated networks to provide a better understanding by implementing these threats and propose relevant mitigating strategies to counteract/reduce the chances of falling victim to these exploits.

Objectives

- To critically evaluate information available about cyber-exploits and research the tools available around these exploits for implementation.
- Based on the Literature Review, select the most appropriate methodology using proven methodologies.
- Using the selected information, demonstrate the implementation of these exploits.
- Based on the outcomes of the implementations, suggest appropriate mitigation strategies and future improvements to enhance security.

3. Implementation

A simulated network was used to capture 3 of the most recent forms of exploitation covered within the research which were Social Engineering, Phishing and Ransomware. The Implementation included the following:

- Real-time Examples
 - Ransomware Infected Server
 - Spear-Phishing Emails
- Physical Implementation of Different Exploits
 - SE through the Social Platform Discord
 - Credential Harvesting Attack
 - Ransomware Simulator
- Kali Linux Operating System

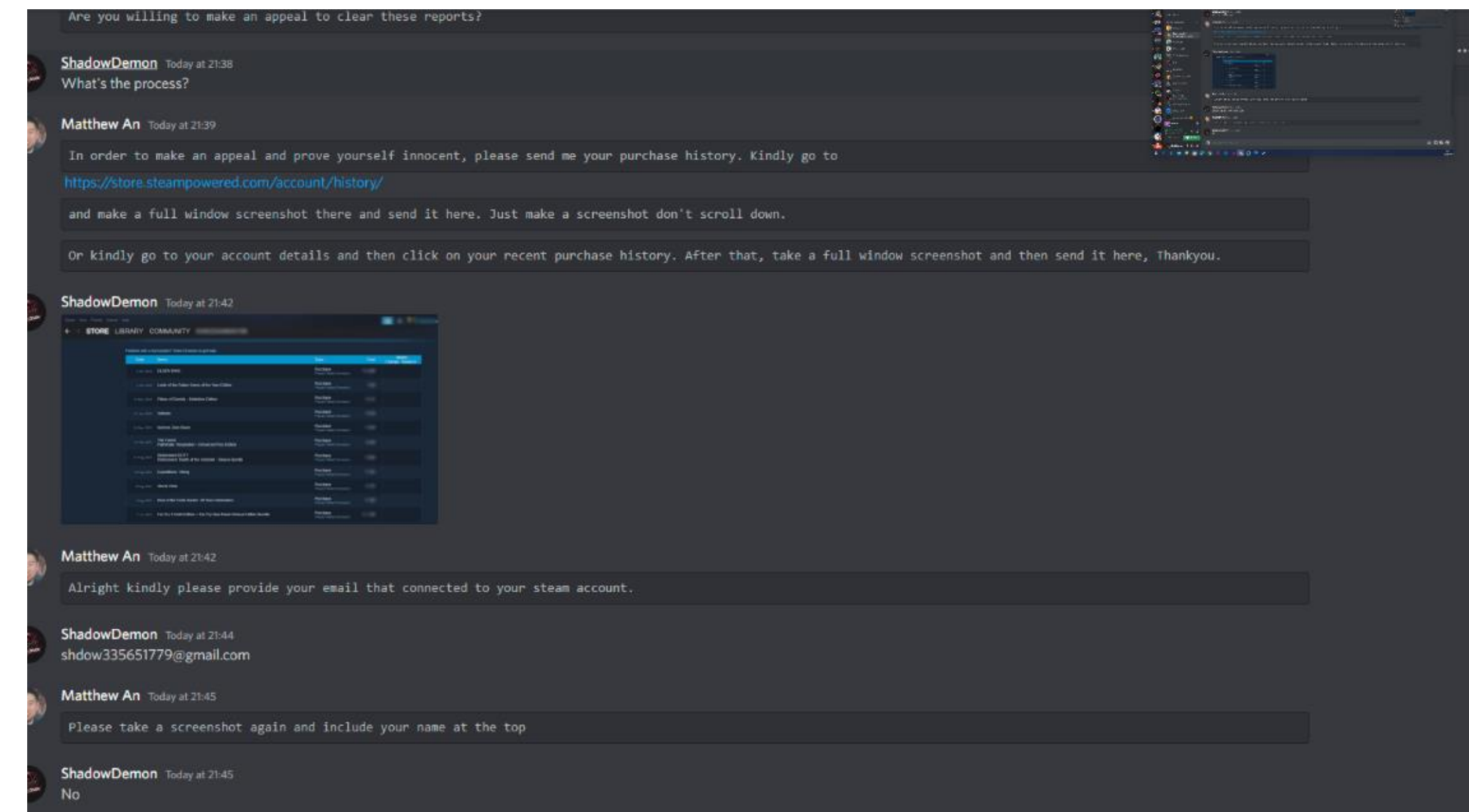


Figure 1 – SE through Discord

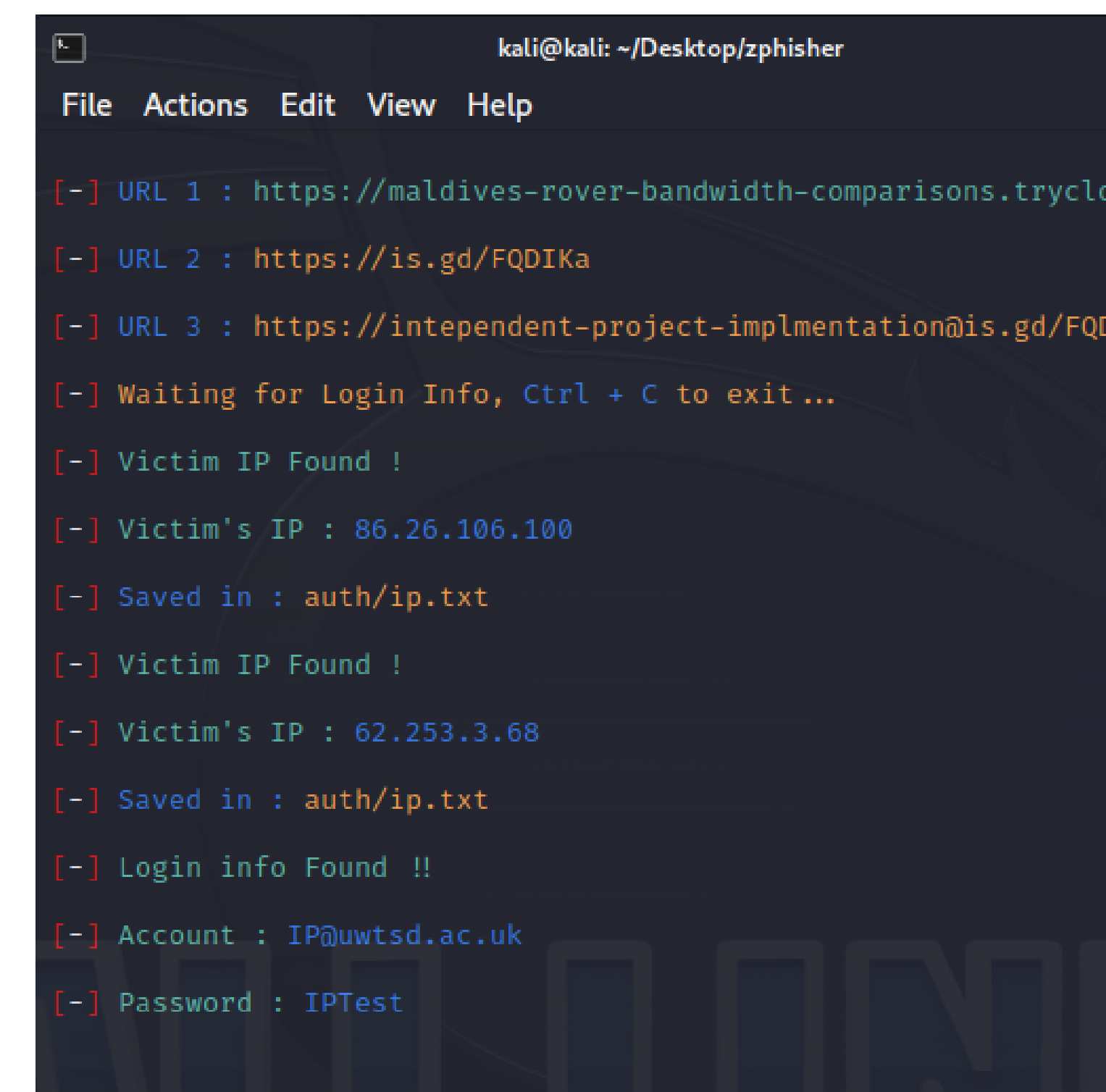


Figure 2 – Captured Credentials

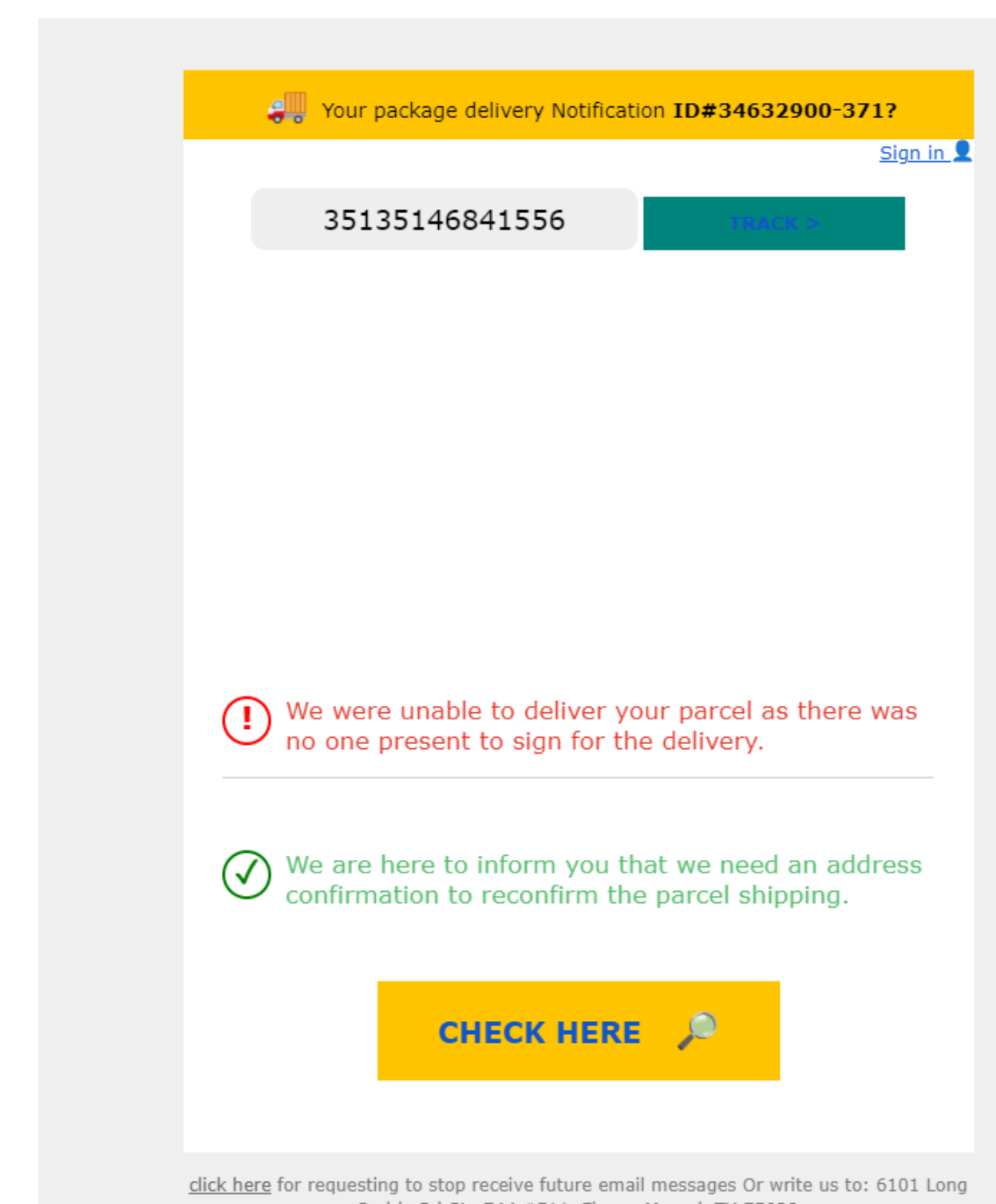


Figure 3 – Phishing Email

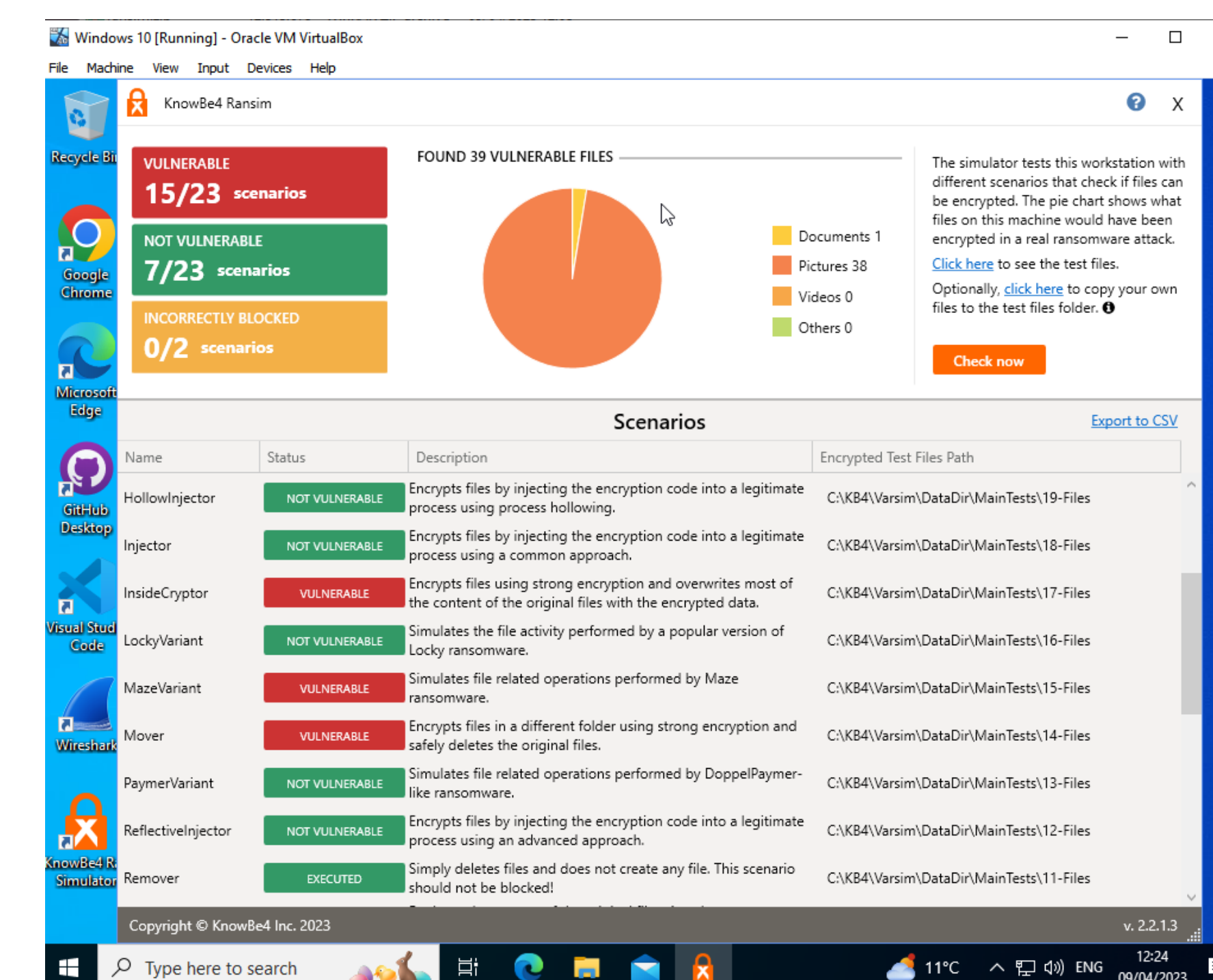


Figure 4 – Ransomware Simulator

4. Mitigation Strategies

In this stage, we engaged in the strategic prioritisation of risks, and the suggestion of cutting-edge measures to mitigate exposure to cyber threats with reference to the implemented exploits covered in the previous sections.

The following Mitigations were suggested as the most suitable:

- User Education [2] – Consistent training sessions on new Social Engineering Exploits etc.
- Advanced Measures such as 2FA and spam filters
- Security and Vulnerability Assessments – This can ensure that any gaps in security can be addressed.
- File Backups and Cloud Services – This can provide greater data security and protection.

5. Conclusion

It is clear from in-depth study and analysis that cyber-attacks offer a serious threat to people, companies, and governments alike. Not all cyberattacks are created equal, and a variety of factors can affect how serious and disruptive they are. Overall, the key to successfully mitigating cyber threats is to implement a comprehensive cybersecurity strategy that includes a combination of technical controls, employee education, and incident response planning. The only way to create an operational environment that is exceptionally safe while cyber threats grow rapidly is to define a countermeasure that includes protection, detection, and response capabilities.

6. Reference List

- Antonyan EA and Grishko NA, 'New Technologies in, Cyber Terrorism Countering', 2020..
- W. P. Nmachi and T. Win, 'Phishing Mitigation Techniques: A Literature Survey', International Journal of Network Security & Its Applications, vol. 13, no. 2, pp. 63–72, Mar. 2021, doi: 10.5121/ijnsa.2021.13205.